EMC® VNX™ Series

Release 1.1

EMC® Secure Remote Support for VNX™

P/N 300-013-445 Rev 02

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Published December 2012

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Corporate Headquarters: Hopkinton, MA 01748-9103

Contents

Preface

As part of an effort to improve and enhance the performance and capabilities of its product lines, EMC periodically releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, please contact your EMC representative.

Special notice conventions

EMC uses the following conventions for special notices:

Note: Emphasizes content that is of exceptional importance or interest but does not relate to personal injury or business/data loss.

NOTICE Identifies content that warns of potential business or data loss.

CAUTION Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

WARNING Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

DANGER Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information—For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to EMC Online Support (registration required) at http://Support.EMC.com.

Troubleshooting—Go to EMC Online Support at http://Support.EMC.com. After logging in, locate the applicable Support by Product page.

Technical support—For technical support and service requests, go to EMC Customer Service on EMC Online Support at http://Support.EMC.com. After logging in, locate the applicable Support by Product page, and choose either **Live Chat** or **Create a service request**. To open a service request through EMC Online Support, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Note: Do not request a specific support representative unless one has already been assigned to your particular system problem.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications.

Please send your opinion of this document to:

techpubcomments@EMC.com

1 Introduction

This chapter introduces you to the EMC Secure Remote Support (ESRS) IP Client for VNX, the ESRS embedded device client on a control station feature, and VG2/VG8 gateway installations.

Major topics include:

ESRS IP Client for VNX overview

You install the ESRS IP Client for VNX software on a monitor station (a host or virtual machine). This software monitors the operation of your EMC® VNX™ for block and legacy (CX, CX3, CX4, and AX4-5 series) systems for error events and automatically notifies your service provider. It also provides a path for your service provider to securely connect to your monitored VNX for block and legacy systems.

The control station in a VNX for file/unified system generates ConnectHome notifications for the block and file portions of the associated system. The ESRS IP Client software allows you to specify control stations that can connect to the monitor station and send ConnectHome notifications through the ESRS communication infrastructure to your service provider. This software also provides a path for your service provider to securely connect to your specified VNX for file/unified system (through the associated control station).

For more information concerning ESRS IP Client for VNX, see Chapter 2.

ESRS embedded device client on a control station overview

The ESRS embedded device client software is packaged into the VNX operating environment (OE) for file/unified systems and resides on the control station. This feature provides your authorized EMC service provider with remote access capabilities to your VNX file/unified system using a secure and encrypted tunnel. For outbound access, the VNX management IP network must allow outbound and inbound HTTPS traffic. The secure tunnel that ESRS establishes between the VNX device and authorized systems on the EMC network can also be used to transfer files out to the VNX system or transfer files back to EMC's network.

For more information concerning this feature, see Chapter 3.

VG2/VG8 installations

Only trained EMC or EMC partner personnel should install and configure a VG2/VG8 gateway configuration. This includes the setup of remote connectivity to contact EMC Customer Service or a third-party service provider for problem resolution assistance.

Note: ESRS IP Gateway 2.0 or later is supported as a remote connectivity and callhome solution for a VG2/VG8 gateway configuration; ESRS Gateway 1.x is not supported.

2

ESRS IP Client for VNX feature

This chapter describes the requirements for installing the ESRS IP Client for VNX software. It explains how to access and download the ESRS IP Client UI-based installer wizard from the EMC Online Support website. It describes how to run the installer wizard that is used to download and configure all the ESRS IP Client software components. These components are required so you can:

- Set up a centralized monitoring environment for your VNX for block or legacy systems
- Specify VNX for file/unified control stations that can connect to the monitor station and send ConnectHome notifications to your service provider.

After completing the installation or upgrade of your ESRS IP Client software on the monitor station, what you do next depends on the type of systems that have been added to your ESRS IP Client configuration.

Major topics include:

ESRS IP Client requirements

Note: Refer to the *EMC ESRS IP Client for VNX Release Notes* for the latest ESRS IP Client environment and systems requirements.

The version of ESRS IP Client software must be at or later than the version of the management software bundled with the VNX Operating Environment (OE) running on each VNX for block or legacy system that is being monitored. Also, legacy Celerra systems are not supported by ESRS IP Client; only VNX for file/unified is supported. ESRS IP Client installation requires:

- **Monitor station**: The monitor station must be a host or virtual machine with a CPU speed of 1.0 GHz or greater, have a total physical memory size of 2 GB or greater and 1 GB of hard disk space, must be running a supported Windows operating system, have the .NET Framework version 2.0 installed, and use the latest JRE version 1.6.0_xx (version 1.6.0_24 or later). The monitor station cannot be a client (host connected to storage-system data ports), and the monitored systems must be able to connect to it over your network. Also, the ESRS IP Client for VNX and the Unisphere Server for Windows cannot coexist on the same server. A pre-installation check in the ESRS IP Client for VNX prevents installation of the ESRS IP Client for VNX on a system that already has the Unisphere Server installed on it. For more information about the monitor station, refer to the *Setting Up a Unisphere Management Station for the VNX Series* document.

  Note: For the latest list of supported Windows operating systems, refer to the *EMC ESRS IP Client for VNX Release Notes*.

  - **If you do not have an existing monitor station** — You can create a monitor station by installing ESRS IP Client on a Windows host.
  - **If you have an existing monitor station running CLARalert (precursor to ESRS IP Client for VNX)** — You can upgrade to the ESRS IP Client on the monitor station. When you perform an upgrade, the ESRS IP Client wizard asks if you want to preserve your existing email configuration or if you want to reconfigure it.
  - **If you have an existing monitor station running event monitor** — You can install the ESRS IP Client on the monitor station.

- **Fixed or static IP address**: The monitor station must have a fixed or static IP address. If dynamic host control protocol (DHCP) is used, you must configure a reserved IP address. The ESRS IP Client wizard automatically detects and configures the ESRS IP Client with the IP address for the monitor station, which is required for the ESRS IP Client installation.
- **Open TCP Ports from the monitor station to your service provider**: The monitor station uses the following TCP ports to connect to your service provider:
  - TCP port 443 (for HTTPS, outbound)

- TCP port 8443 (for HTTPS, outbound); not required for functionality, however without this port being opened there will be a significant decrease in remote support performance.

- **Open TCP Ports from the monitor station to your storage systems**: The monitor station uses the following TCP ports to connect to the storage systems:
  - TCP port 80 (for HTTP, inbound/outbound)
  - TCP port 443 (for HTTPS, inbound/outbound)
  - TCP port 25 (for the SMTP server, outbound)
  - TCP port 6389 (for the Unisphere Host Agent, outbound)
  - TCP port 5414 (for the EMCRemote Client, outbound)
  - TCP port 9519 (for RemotelyAnywhere on CX4 systems running EMC FLARE® version 04.29 or later, or on VNX for block systems, outbound)
  - TCP port 6391, 6392, and 60020 (for the Remote Diagnostic Agent, outbound)
  - TCP port 22 (for the CLI with SSH)
  - TCP port 13456 (for KTCONS)
  - TCP port 22 and 9519 (for RemoteKtrace)
  - TCP port 80, 443, 2162, 2163, and 8000 (for Unisphere Service Manager, Unisphere, and Navisphere® Secure CLI)

- **Proxy server**: If the monitor station connects to the Internet through a proxy server, you must indicate this during the ESRS IP Client installation and provide the IP address, port, and protocol (HTTPS or SOCKS) for the proxy server. If the proxy server requires authentication (SOCKS is supported only with authentication), you must also indicate this during installation and supply login credentials for the proxy server. You must supply both a username and password for authentication.
- **EMC Online Support account**: You must have an existing and proper EMC Online Support account. You are required to log in to the EMC Online Support website at http://Support.EMC.com and supply your valid storage-system serial number before you can download and install the ESRS IP Client software.
- **Registered monitoring site**: The monitoring site must be registered on EMC Online Support. During the ESRS IP Client installation, you must specify contact information that includes the name, email address and phone number of a person to contact at the monitoring site.
- **Portal system**: A storage system through which you can centrally monitor specified storage systems in a domain for storage system events. The portal system must be a VNX for block or legacy system running the latest VNX Operating Environment (OE) version that is running on the VNX for block or legacy systems it is monitoring. During the ESRS IP Client installation, you must provide the IP address for one of the portal system's storage processors (SP) and the portal system's global administrator login credentials.

Note: If your ESRS IP Client installation will use the optional email notification, for example, as a backup communication method for the Call Home feature, you will need connectivity to an outgoing SMTP server. During ESRS IP Client installation, you must provide the IP address for the SMTP server and your email address (in the `from` field) for email notification.

New installation

For a new ESRS IP Client installation, the InstallAnywhere wizard automatically installs a communication infrastructure that supports secure inbound/outbound communication (SSL) as the primary communication method with your service provider. This communication

infrastructure notifies your service provider of events (Call Home feature, see Figure 1 on page 13).

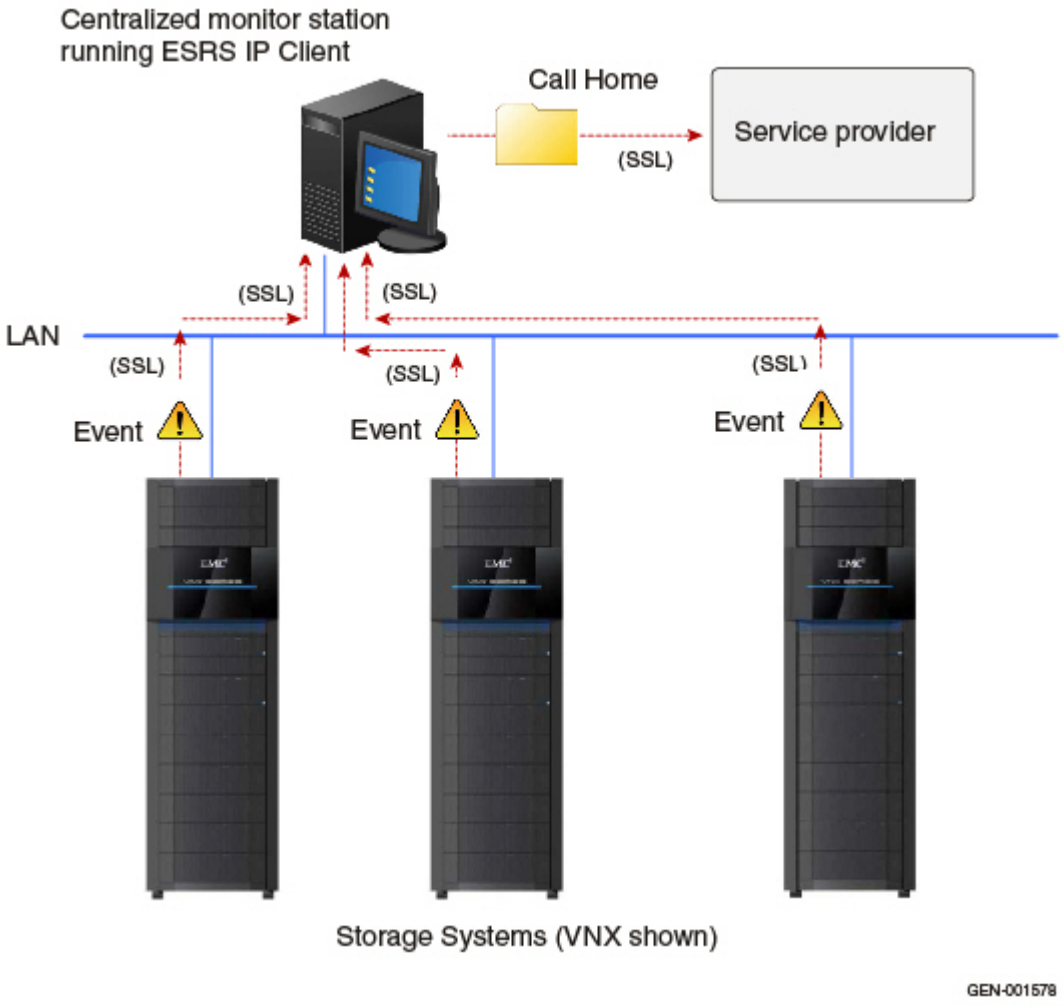

Figure 1. ESRS IP Client communication infrastructure - Call Home example

This same communication infrastructure provides your service provider with remote access to your monitored VNX for block and legacy systems (see Figure 2 on page 14).

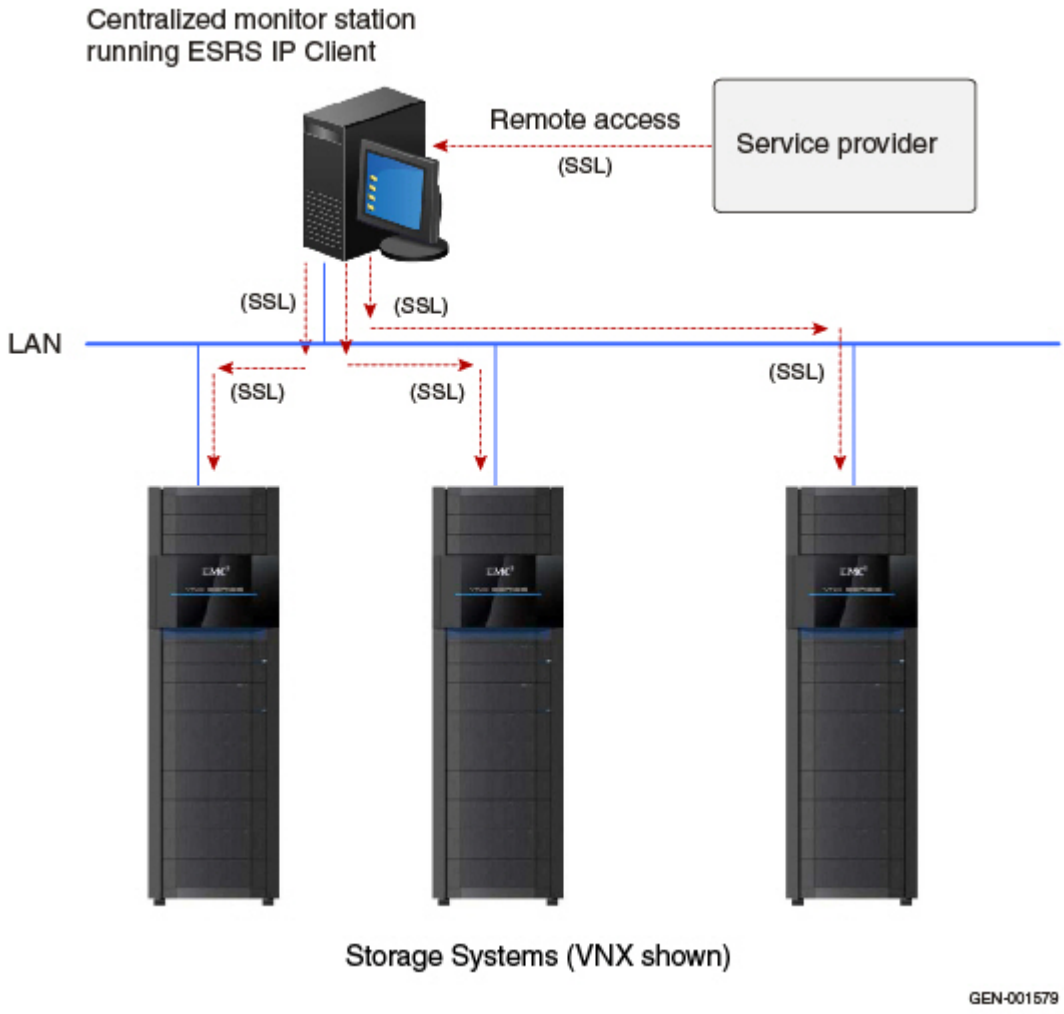

Figure 2. ESRS IP Client communication infrastructure - Remote access example

Also, this same infrastructure is used to send ConnectHome data from your specified VNX for file/unified device(s) (the associated control station(s) that are connected to the monitor station) to your service provider and to provide your service provider with remote access to your VNX for file/unified devices.

Note: The default authorization permission for remote access to your VNX for file/unified or your monitored VNX for block or legacy systems is set to **always allow**. If you require more control over remote access to your VNX for file/unified or your monitored VNX for block or legacy systems, you can use a Policy Manager to set authorization permissions. The Policy Manager software component is installed on a customer-supplied server. It controls remote access to your devices, maintains an audit log of remote connections, and supports file transfer operations. You can control who, what, and when, and even why access to your system has occurred. For additional information on Policy Manager, go to the EMC Online Support website (Support.EMC.com). After logging in, locate the applicable Support by Product page and the link for the specific product technical documentation.

During the ESRS IP Client software installation, you can select to use email as your backup communication method for the Call Home feature and to notify you when events are sent from your monitored VNX for block and legacy systems to your service provider. Also, you designate the monitor station and portal system to configure your centralized monitoring environment. The VNX for block system that you designate as a portal system is automatically added to the list of monitored systems.

Upgrade

For upgrades from either CLARalert or ESRS IP Client for CLARiiON® software to ESRS IP Client for VNX software, you can choose to keep your existing communication configuration (such as dial-up or email) for the Call Home feature under the following conditions:

Note: This option is not available when either ESRS IP Client for VNX or ESRS IP Client for CLARiiON software and the associated communication infrastructure have been installed.

- You are upgrading from CLARalert software (version 6.22 or later) to ESRS IP Client for VNX
- You are upgrading from ESRS IP Client for CLARiiON to ESRS IP Client for VNX after you previously upgraded from CLARalert software (version 6.22 or later) to ESRS IP Client for CLARiiON and kept the existing communication configuration (such as dial-up or email) for the Call Home feature.
- Your service provider set up your previous ESRS IP Client for CLARiiON communication configuration with dial-up or email for the Call Home feature and you are upgrading from that to the ESRS IP Client for VNX.

This option allows you to continue to use your existing communication configuration (such as dial-up or email to your service provider) for the Call Home feature (for VNX for block and legacy systems). All your central monitoring software will be upgraded; however, the ESRS communication infrastructure will not be automatically installed during the upgrade. If such an option is selected, you cannot add a VNX for file/unified system into the ESRS IP Client configuration because the required ESRS communication infrastructure is not installed. If you choose not to keep your existing dial-up or email configuration, the upgrade is treated as a new ESRS IP Client installation.

EMC does not recommend using dial-up or email as the primary Call Home communication method. EMC recommends using the ESRS communication infrastructure that can be automatically installed on the monitor station.

CAUTION The customer installation mode does not support the installation of the ESRS IP Client for VNX for block or legacy systems with a distributed (noncentralized) monitoring environment. If you have an existing Call Home configuration that uses a distributed monitoring environment, the upgrade will create a centralized monitoring environment (see Figure 1 on page 13). The existing distributed monitoring environment and newly created centralized monitoring environment can result in duplicate notifications to your service provider. Your existing distributed monitoring environment will not be upgraded. You or EMC authorized service provider should turn off distributed monitoring on all VNX for block or legacy systems that will be included in your centralized monitoring environment before installing the ESRS IP Client software.

The customer installation mode requires a centralized monitoring environment. In a centralized monitoring environment you designate a monitor station that generates Call Home notifications for the VNX for block and legacy systems that it monitors for events. The centralized monitoring environment is an option with the Navisphere® Manager or Unisphere™ application.

Verify HTTPS connectivity during pre-installation

The ESRS IP Client installer wizard verifies the following IP address names for HTTPS connectivity during pre-installation:

ESRS Core (for gateway pings): esrs-core.emc.com

ESRS UI (user interface for ServiceLink Access, EMC's service site): esrs.emc.com

Global access server:

- esrgweprd01.emc.com
- esrgweprd02.emc.com
- esrgweprd03.emc.com
- esrghoprd01.emc.com
- esrghoprd02.emc.com
- esrghoprd03.emc.com
- esrgckprd01.emc.com
- esrgckprd02.emc.com
- esrgckprd03.emc.com
- esrgscprd01.emc.com
- esrgscprd02.emc.com
- esrgscprd03.emc.com

- esrgspprd01.emc.com
- esrgspprd02.emc.com
- esrgspprd03.emc.com

HTTPS connectivity is required for the ESRS core and ESRS UI IP address names and at least four of the global access server IP address names. EMC recommends that all the global access server IP address names listed above should be accessible for HTTPS connectivity.

InstallAnywhere wizard

Note: The InstallAnywhere wizard will prompt you to select an installation mode for ESRS IP Client. This document describes the customer installation mode only. It is the recommended installation mode and is supported for customers performing a new ESRS IP Client installation or upgrade.

The InstallAnywhere wizard guides you through the ESRS IP Client installation process and, if required, provides context-sensitive help on how to perform a particular step. You can use the wizard for a new ESRS IP Client installation, or to upgrade an existing 6.22 or later CLARalert or ESRS IP Client for CLARiiON environment. An EMC authorized service provider must perform upgrades to an existing CLARalert environment that is running a CLARalert version earlier than 6.22.

Download and install ESRS IP Client software

You can access and download the ESRS IP Client UI-based installer wizard from the EMC Online Support website. Use the wizard to download and configure all the ESRS IP Client software components required to set up a centralized monitoring environment for your VNX for block or legacy systems and to specify VNX for file control stations that can connect to the monitor station and send ConnectHome notifications to your service provider.

Before you begin

Do not install the ESRS IP client for VNX on an ESRS gateway server.

Before installing the ESRS IP client for VNX on a Windows 7 host with the Windows firewall enabled, ensure TCP/IP port 6389 is open. TCP/IP port 6389 must be open to allow the Unisphere Host Agent to function properly. If TCP/IP port 6389 is blocked, the installation will fail because the client will not be able to communicate with the target storage systems. The HostAgent.exe is located at `C:\Program Files\EMC\HostAgent\HostAgent.exe` for 32 bit Windows versions and `C:\Program Files (x86)\EMC\HostAgent\HostAgent.exe` for 64 bit Windows versions.

Also, the ESRS IP Client for VNX and the Unisphere Server for Windows cannot coexist on the same server. A pre-installation check in the ESRS IP Client for VNX will prevent installation of the ESRS IP Client for VNX on a system that already has the Unisphere Server installed on it. If this is the case, uninstall the Unisphere Server before installing the ESRS IP Client for VNX. The ESRS IP Client for VNX uses the presence of the registry key `HKEY_LOCAL_MACHINE\Software\EMC\ManagementServer` to determine if the Unisphere

Server is installed. If that key is not removed by the Unisphere Server uninstaller, it can prevent the ESRS IP Client for VNX from being installed. You can delete the key from the registry by using regedit and then you should be able to install the ESRS IP Client for VNX.

Procedure

From the monitor station:

1. Go to the EMC Online Support website at http://Support.EMC.com and locate the Download page and the link to download the ESRS IP Client for VNX software.
2. Select **Download ESRS IP Client** and save the software to your monitor station.
3. In the folder where you saved the ESRS IP Client, double-click the ESRS IP Client executable file or if necessary, right-click the file and select **Run as** to run the installation wizard using a different user's credentials.
4. Follow the steps in the wizard to complete the installation.

Note: For all CX4 systems that are running FLARE version 04.29 or later and VNX for block systems and that are deployed in this ESRS IP Client configuration, you must add the monitor station IP address to the RemotelyAnywhere filter tables of those systems. See Add monitor station to RemotelyAnywhere IP address filter tables on page 18 for detailed information.

For a list of the IP address names verified for HTTPS connectivity during the pre-installation checks, see Verify HTTPS connectivity during pre-installation on page 16. Also, the ESRS IP Client software installation generates four log files. Two of these log files (`esrsagent_installer.log` and `esrsipclient_installer.log`) are located under the user's home directory in the `EMC\ESRSIPClient` folder. The other two logs, `esrs_rscapi.log`, and `esrs_jema.log`, are located in the directory where the ESRS IP Client is installed. The `esrs_rscapi.log` log is created for VNX for block registrations only. The `esrs_jema.log` log is created for VNX for file registrations only.

Add monitor station to RemotelyAnywhere IP address filter tables

---

Note: Perform this procedure only for all CX4 systems running FLARE version 04.29 or later and all VNX for block systems in this ESRS IP Client configuration.

By default, this feature adds an always-on, additional layer of security that restricts the use of remote service tools to the system's service ports. Administrators and security administrators can extend remote service tool access to a system's management ports by entering the IP addresses of the attached, trusted service clients.

Note: For IPv6 configurations, temporary private addresses are disabled on the system by default. EMC strongly recommends that you also disable them on the client system.

---

1. Enter the SP A or SP B IP address or hostname in a supported browser address field and append the setup page path to the IP address or hostname, for example, `http://IP address/setup` or `http://hostname/setup`.

   The SP setup login page opens.

2. Enter the system Navisphere Manager or Unisphere administrator access username and password.

   The SP setup page opens.

3. Scroll down to **Set RemotelyAnywhere Access Restriction** and click the name panel to open the page.

   Note: System security must be enabled and configured before you can access the Set RemotelyAnywhere Access Restriction IP address filter table.

   The **IP Filter Configuration for RemotelyAnywhere** page opens.

4. Verify that your monitor station IP address is entered in the IP address filter tables.

5. Enter your monitor station IP address in the **Filters that apply to all storage systems in the domain** input table.

   Note: You can enter up to 16 RemotelyAnywhere (RA) client addresses into the input tables. At this time you cannot enter address ranges or complete subnets into the input tables. Entering RA client addresses into the Connected storage system only input table does not propagate those addresses to all CX4 systems in the domain that are running FLARE version 04.29 or later and all VNX for block systems in the domain. Use the Connected storage system only input table if you do not want to propagate the data to other systems in the domain.

   Using the **Filters that apply to all storage systems in the domain** input table will propagate the RA client address you entered to all CX4 systems in the domain that are running FLARE version 04.29 or later and all VNX for block systems in the domain.

6. Click **Apply Setting**.

   Note: Updating the IP filter tables will reset any existing RA connections.

   The **RemotelyAnywhere IP Filter Configuration - Confirmation** page opens.

7. Click **Apply Settings**.

Note: The following text message should appear:

```
RemotelyAnywhere IP Filter request was successful.
```

The **RemotelyAnywhere IP Filter Configuration - Apply** page opens.

8. Click **Back**.

   The main setup page appears.

9. Click **Logout** and close the browser.

10. If you entered the monitor station IP address in the **Connected storage system only** filter table, repeat these steps for all other CX4 systems in the domain that are running FLARE version 04.29 or later and all other VNX for block systems in the domain of this ESRS IP Client configuration.

Change HTTPS communications security

When you initially set up a configuration with VNX for file/unified systems, the HTTPS connection between the ConnectHome feature on a control station and the ESRS HTTPS Listener service that is installed on the monitor station uses a default HTTPS configuration. Once the ConnectHome feature and the ESRS HTTPS Listener service are installed and configured using the default HTTPS configuration and the connection is working, you should provide the ESRS HTTPS Listener service with an X.509 certificate that is specific to the system hosting the service. This action strengthens the security of the HTTPS connection and allows the server identity to be verified by any ConnectHome client. For specific instructions and additional information, go to the EMC Online Support website and locate the applicable Support by Product page and the link for the specific product technical documentation (*Managing the SSL Certificate for the ESRS HTTPS Listener Service*).

Make changes using Unisphere UI

Use the Unisphere UI to do the following:

- Add VNX for block and legacy systems to or remove them from your centralized monitoring environment.
- View the properties of the Call Home templates and assign additional Call Home templates to VNX for block or legacy systems.
- Manage ConnectHome information for a VNX for file/unified system.
- View events for a monitored VNX for block or file/unified or a legacy system.

For more information about using Unisphere, see the Unisphere help, which is in the Unisphere UI or go to the EMC Online Support website and locate the applicable Support by Product page and the link for the specific product technical documentation required. The website has the most recent version.

Make changes using regtool CLI tool

When the ESRS IP Client software is downloaded, the regtool CLI tool is installed in the directory where the ESRS IP Client is installed.

Use the **regtool** CLI tool to do the following:

- Register newly added VNX for file systems with the ESRS IP Client and set up ConnectHome notifications from these systems through the monitor station.
- Complete Event Monitor configuration if the ESRS IP Client software was installed with only VNX for file systems and subsequently a VNX for block or legacy system needs to be added to the monitor station.

After completing the installation of your ESRS IP Client software on the monitor station, you must use the regtool CLI tool to add VNX for file/unified systems and the Configtool executable file to remove VNX for file/unified systems. The Configtool executable file is located in the directory where the ESRS IP Client is installed.

Note: For additional information on Configtool, go to the EMC Online Support website at http://Support.EMC.com. After logging in, locate the applicable Support by Product page and the link for the specific product technical documentation.

You must use Unisphere to add or remove VNX for block or legacy systems unless none were added when you installed the ESRS IP Client. If you installed the ESRS IP Client with only VNX for file/unified systems, and subsequently you need to configure it to monitor VNX for block or legacy systems, use the regtool CLI tool to add the first VNX for block or legacy system and then use Unisphere to make further VNX for block or legacy system changes. When you add a VNX for block or legacy system using regtool, it adds all the VNX for block and legacy systems in the domain that it discovers. Regtool assigns the first system that it finds in the domain which is connected and running the highest version of Unisphere as the portal system. The portal URL shortcut on the desktop updates to point to this system. You require a portal system to use Unisphere to make further VNX for block and legacy system changes.

The **regtool** command requires the type of system being added, its IP address and login username and password as arguments. Regtool command syntax is as follows:

```
regtool -a ( -c <ipaddress>[:<port>] | -s <ipaddress>[:<port>] ) -u
<username> -p <password> [-v]
```

-a Add a control station or a storage processor. You can add a storage processor with this utility only if storage processors have not been added to this system's monitoring configuration. You must use Unisphere on the portal system to add additional storage processors.

-c Option for control station IP address

or

-s Option for storage processor IP address

The IP address can optionally include a port number. If the IP address does not include a port number, it will default to 22 for a control station and 443 for a storage processor.

-u Option for username of a user with Administrator access on the system

-p Option for password

-v Prints verbose output

The following command displays the help message for **regtool**:`regtool -h`

The possible return values for the **regtool** command are as follows:

`0` Success

`<0` Error

`-1` Syntax Error

`-2` Insufficient arguments

`-99` Unexpected error

The posible error messages for the **regtool** command are as follows:

```
Error: Invalid system type.

Error: Use Unisphere on the portal system at {0} to add additional storage
processors.

Error: Unrecognized option: {0}

Error: Command not recognized.

Error: Insufficient parameters specified.

Error: Password must be specified.

Error: Username must be specified.

Error: IP address must be specified.

Error: Only one system type and IP address can be specified at the same
time.
```

The location of the **regtool** log file is:

```
<User's Home Directory>\EMC\ESRSIPClient\esrsipclient_regtool.log
```

The regtool command requires elevated or administrative privileges. To run regtool on a system operating with Windows Vista® 2007 or 2008, you should use the Run as administrator command:

1. Click **Start**.
2. In the **Search** dialog box, type `command prompt`.

3. In the list of results, right-click **Command Prompt**, and then click **Run as administrator**.
4. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

3

ESRS device client on control station feature

This chapter describes the requirements for the ESRS embedded device client on control station software and provides an operational description of the feature. The chapter also describes the processes to provision the feature and to re-provision the feature.

Major topics include:

ESRS embedded device client on control station requirements

The ESRS embedded device client on control station feature requires the following:

- VNX operating environment (OE) for VNX version 7.1.56.x or later.
- At least one DNS server must be configured on your VNX before you set up the ESRS communication channel and provision the feature; otherwise, the feature will not work.
- Unrestricted access to *.emc.com over the Internet using HTTPS (for non-proxy environments).
- EMC online support account.

Note: Provisioning or re-provisioning the ESRS device client on a control station in a VNX file/unified system requires an active account on the EMC Online Support website. This account associates specific credentials with a particular organization and email domain. When you provision or re-provision the ESRS device client on a control station in a VNX file/unified system, you must specify these credentials (a user name password pair) to set up the ESRS communication channel for the system.

The following requirements are dependent on your ESRS device client on a control station implementation:

- If your ESRS implementation will include a proxy server to connect to the Internet, you must indicate this when you provision the ESRS feature.
- If your ESRS implementation will include a Policy Manager for more control over remote access to your VNX system, you must indicate this when you provision the ESRS feature.
- If your ESRS implementation will include a proxy server for your VNX to connect to a Policy Manager, you must indicate this when you provision the ESRS feature.

ESRS embedded device client operational description

The ESRS embedded device client on control station feature provides an IP-based connection that enables EMC Support to receive error files and alerts from your VNX file/unified system, and to perform remote troubleshooting resulting in a fast and efficient time to resolution.

Note: EMC strongly recommends that you provision the ESRS device client on control station feature and select it as the primary transport mechanism for Connect Home notifications. These actions will help to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. If you do not provision ESRS, you may need to collect system information manually to assist EMC Support with troubleshooting and resolving problems with the VNX file/unified system.

The ESRS device client on control station feature offers a secure architecture from end to end, including the following features:

- EMC issues X.509 digital certificates to authenticate the ESRS device client on control station to EMC.

- EMC professionals are authenticated using two unique factors.
- All EMC service professionals have a unique username that is logged with all their actions.
- All communication originates from the control station. The ESRS device client on control station does not accept unsolicited connections from EMC or the Internet.
- All communications between EMC and the ESRS device client on control station includes the latest security practices and encryption technologies, including certificate libraries based on RSA Lockbox technology, and Advanced Encryption Standard (AES) 256-bit encryption.
- Those who implement the ESRS device client on control station solution can further control remote access by using the Policy Manager. The Policy Manager gives full control of how EMC interacts with VNX systems. SSL is available between the ESRS device client on control station and the Policy Manager.

ESRS device client on control station management

You can manage the ESRS device client on control station feature using Unisphere. You can provision or re-provision the service, set up a proxy server or Policy Manager, or both. You must provide your support account credentials to provision or re-provision the ESRS device client on a control station.

The VNX file/unified system itself does not implement any policies. If you require more control over remote access to your VNX file/unified system, you can use a Policy Manager to set authorization permissions. The Policy Manager software component can be installed on a customer-supplied server. It controls remote access to your devices, maintains an audit log of remote connections, and supports file transfer operations. You can control by whom, what, and when access to your VNX file/unified system occurs. For additional information about the Policy Manager, go to the EMC Online Support website

(Support.EMC.com). After logging in, locate the applicable Support by Product page and search for the link to the specific ESRS product technical documentation.

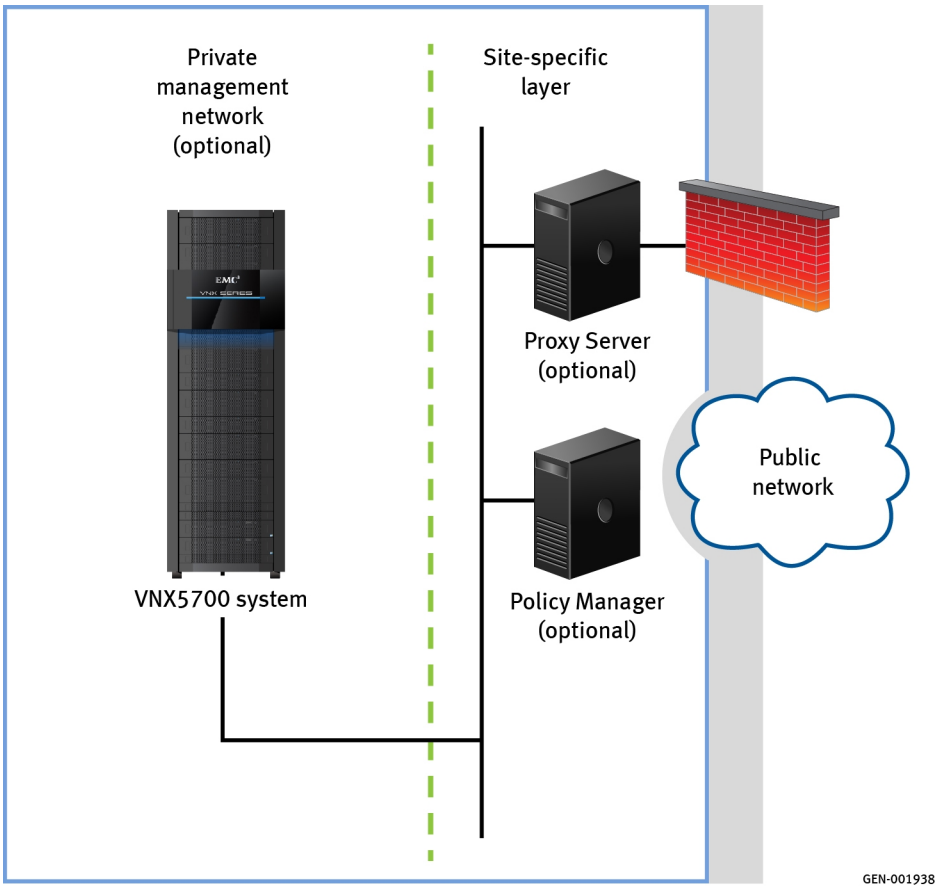

Figure 3. ESRS device client on control station feature customer-side network topology example

ESRS device client on control station communication

Although a VNX file/unified system can be configured with DNS disabled, access to a DNS server is required for the ESRS device client on control station feature to work. You should set the ESRS device client on control station feature to be the primary (default) method used by ConnectEMC to communicate with EMC backend systems.

Provision ESRS embedded device client on control station

Note: As a prerequisite for you to provision the ESRS device client on control station feature in your VNX file/unified system, you must have an existing EMC Online Support account. Also, at least one DNS server must be configured on your VNX before you set up the ESRS communication channel and provision the feature; otherwise, the feature will not work.

You or your EMC service provider can provision the ESRS device client on the control station through either the VNX Initialization Assistant (VIA, for fresh installs) or Unisphere. To provision the feature requires either you to provide your EMC Online Support account credentials (username and password) or your EMC service provider to provide their SecurID credentials.

To provision the ESRS device client on control station feature in Unisphere, you must be logged in to the control station as User root and Scope Local. Select your system and from the task list, under **Service Tasks**, select **Manage ESRS for File**.

Note: For a VNX with two control stations, a dialog box for selecting the target control station (Primary or Standby) appears first. The Primary control station will be selected by default. If necessary, you can change the selection and click Continue to navigate to the Manage ESRS page for the corresponding control station. Also, as an alternate method to access the ESRS parameters, under Service Tasks, you can select Manage Connect Home for File and click Manage ESRS Settings in the ESRS Priority field. This link navigates directly to the Manage ESRS page for the primary Control Station. To manage the ESRS on a standby control station, you must select Manage ESRS for File from the task list under Service Tasks.

When provisioning the ESRS device client on the control station, you can provision an optional Proxy Server or a Policy Manager, or both. Once you have provisioned the feature, you should set **ESRS** as the primary transport mechanism for Connect Home notifications. You can do this by selecting your system and from the task list, under **Service Tasks**, select **Manage Connect Home for File**. After you configure your Connect Home settings, you should test them using **Test** on the **Manage Connect Home** page.

For detailed instructions and more information about provisioning the ESRS device client on control station feature and testing the transport mechanisms for Connect Home notifications, see the Unisphere online help.

Proxy Server

If the VNX file/unified system will use a proxy server to connect to the Internet, you must indicate this when you configure the ESRS. You must provide the following information for the proxy server:

- Protocol (HTTPS or SOCKS)
- IP address
- Port number

If the proxy server requires authentication (SOCKS is supported only with authentication), you must also indicate this during the ESRS configuration and supply login credentials for the proxy server. You must supply both a username and password for authentication.

If you install a proxy server on a non-standard port, you will need to enter a port number to use the proxy server. If the port is not specified, the system defaults to the appropriate standard port for the given proxy type.

Policy Manager

If the VNX file/unified system will use a Policy Manager to set authorization permissions, you must indicate this when you configure the ESRS. You must provide the following information for the Policy Manager:

- Indicate whether the connection to the Policy Manager needs to be secure (SSL will be used in the connection to the Policy Manager); otherwise, SSH is used in the connection to the Policy Manager.
- IP address
- Port number

If the Policy Manager will use a proxy server to connect to the VNX file/unified system, you must indicate this when you configure the ESRS. You must provide the following information for the Policy Manager's proxy server:

- Protocol (HTTPS or SOCKS)
- IP address
- Port number

If the Policy Manager's proxy server requires authentication (SOCKS is supported only with authentication), you must also indicate this during the ESRS configuration and supply login credentials for the proxy server. You must supply both a username and password for authentication.

When installing a policy manager, you have the option to change the default port if you choose to use a non-secure transport. In this case, you will need to enter a port number for the policy manager proxy server. If you do not specify the port, then a default port is used. Default ports are 8443 for secure communication or 8090 if not secure.

Re-provision ESRS embedded device client on the control station

Note: As a prerequisite for you to re-provision the ESRS embedded device client on the control station in your VNX file/unified system, you must have already provisioned the ESRS feature. Also, to re-provision the ESRS device client on control station feature in Unisphere, you must be logged in to the control station as User root and Scope Local. See Provision ESRS embedded device client on control station on page 29 for information.

You may need to re-provision the ESRS device client on the control station feature for any of the following reasons:

- To add or remove a Proxy Server or change existing Proxy Server settings
- To add or remove a Policy Manager or associated Proxy Server or change existing Policy Manager settings, including settings for an associated Proxy Server

Upgrade ESRS embedded device client on control station

The ESRS embedded device client on control station feature is packaged into the VNX file/unified software image. Upgrade of the device client or associated features will only be delivered as part of a full VNX file/unified system software upgrade.

Index